

Increasing the security of the ping-pong protocol by using many mutually unbiased bases

Piotr Zawadzki*

*Institute of Electronics, Faculty of Automatic Control, Electronics and Computer Science,
Silesian University of Technology, Akademicka 16, 44-100 Gliwice*

Zbigniew Puchała† and Jarosław Adam Miszczak‡

*Institute of Theoretical and Applied Informatics,
Polish Academy of Sciences, Bałtycka 5, 44-100 Gliwice, Poland*

In this paper we propose an extended version of the ping-pong protocol and study its security. The proposed protocol incorporates the usage of mutually unbiased bases in the control mode. We show that, by increasing the number of bases, it is possible to improve the security of this protocol. We also provide the upper bounds on eavesdropping average non-detection probability and propose a control mode modification that increases the attack detection probability.

Keywords: quantum cryptography, quantum secure direct communication, ping-pong protocol

I. INTRODUCTION

A method of quantum secure direct communication (QSDC), contrary to quantum key distribution (QKD) schemes, offers the confidential exchange of deterministic messages without key agreement [12]. The interest in this fascinating idea started a decade ago in seminal papers of Beige *et.al.* [1] and Boström *et.al.* [2]. Since then QSDC techniques have been developed following two different paradigms: exploiting indistinguishability of non-orthogonal quantum states [1, 4, 14, 17, 22] and based on entanglement of signal particles with a system inaccessible to the eavesdropper [2, 6, 18, 25]. The protocols from the former family are usually simpler to implement at the price of classic channel utilization in message mode, although exceptions of this rule exist [14]. On the other hand, the entanglement based ping-pong protocol uses classic channel only in control mode [2]. This feature can be exploited to build an additional cryptographic security layer which improves security of the protocol [20, 24]. The ping-pong protocol has been also improved and extended in other directions including super-dense information coding [5, 21] and its variants based on higher dimensional signal particles [19, 23]. However, in the analyses of higher dimensional variants it was assumed that control mode is executed in at most two dual bases. This possibly understates an eavesdropping detectability.

The main aim of this paper is to show that, by increasing the number of bases used in the control mode, it is possible to decrease an upper bound of the attack non-detection probability. Eavesdropping is most effectively detected if subsequent tests are executed in randomly selected mutually unbiased bases (MUB) [8]. Unfortunately, the problem of finding MUB for the arbitrary

Hilbert space remains unsolved and constructive solutions exist only for spaces of dimension $N = p^m$ where p is prime [7, 10] and/or spaces with dimension not exceeding six [3, 15].

II. PRELIMINARIES

A. Mutually Unbiased Bases

A sequence of orthonormal bases $\{\mathcal{B}^{(0)}, \mathcal{B}^{(1)}, \dots, \mathcal{B}^{(M)}\}$ of \mathbb{C}^N is called MUB if, for any two elements $|b_k^{(m)}\rangle \in \mathcal{B}^{(m)}, |b_l^{(n)}\rangle \in \mathcal{B}^{(n)}$, the following condition holds

$$|\langle b_k^{(m)} | b_l^{(n)} \rangle|^2 = \delta_{m,n} \delta_{k,l} + \frac{1}{N} (1 - \delta_{m,n}), \quad (1)$$

where N denotes the dimension of underlying Hilbert space. The explicit construction of MUB is only known in the case of dimension $N = p^m$, where p is a prime and m is a positive integer [7]. For an odd prime p we have [7]

$$\begin{aligned} |b_k^{(l)}\rangle &= \sum_{q=0}^{N-1} B_{k,q}^{(l)} |b_q^{(0)}\rangle \\ &= \frac{1}{\sqrt{N}} \sum_{q=0}^{N-1} \omega^{\ominus k \odot q} \omega^{(l-1) \odot q \odot q \odot 2} |b_q^{(0)}\rangle, \end{aligned} \quad (2)$$

where $\omega = e^{2\pi i/N}$, circled operations \odot , \oslash , \ominus denote multiplication, division and subtraction in the finite field $\text{GF}(p^m)$ respectively and $|b_q^{(0)}\rangle$ are vectors of computational basis. In the case of $p = 2$ the explicit formulas for the MUB elements are more involved [10].

*Electronic address: piotr.zawadzki@polsl.pl

†Electronic address: z.puchala@iitis.pl

‡Electronic address: miszczak@iitis.pl

B. Ping-pong protocol operation

Bob, the recipient of information, prepares an EPR pair composed of qudits [9]

$$|\psi_{0,0}\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |b_k^{(0)}\rangle |b_k^{(0)}\rangle. \quad (3)$$

One of the qudits, referred to as 'home', is kept confidential, while the second one, called 'travel', is sent to Alice. Because of an entanglement, Alice's manipulations on the travel qudit induce non-local effects. Alice is able to encode $2 \log_2 N$ bits of information per one protocol cycle applying one of the unitary transformations

$$U_{\mu,\nu} = \sum_{k=0}^{N-1} \omega^{\mu k} |b_{k+\nu}^{(0)}\rangle \langle b_k^{(0)}|, \quad (4)$$

where $\mu, \nu = 0, \dots, N-1$. Operator (4) transforms the initial state into another EPR pair $|\psi_{\mu,\nu}\rangle$ [13] which can be unambiguously discriminated by Bob when the 'travel' qudit is returned by Alice. Eavesdropping Eve cannot distinguish the travel qudit on its way forth and back from a maximally mixed state

$$\rho_t = \frac{1}{N} \sum_{\alpha=0}^{N-1} |b_\alpha^{(0)}\rangle \langle b_\alpha^{(0)}|, \quad (5)$$

so this way she cannot infer any information about the encoding operation used by Alice. Because of that indistinguishability, further analysis can be carried out as if Bob sent one of the randomly selected states $|b_\alpha^{(0)}\rangle$ [2]. However, Eve can entangle the 'travel' qudit with some ancilla system before it reaches Alice

$$|\psi_\alpha\rangle = A|b_\alpha^{(0)}, \phi\rangle = \sum_{l=0}^{N-1} a_{\alpha,l} |b_l^{(0)}\rangle, \phi_{\alpha,l}\rangle, \quad (6)$$

where $\alpha = 0, \dots, N-1$ and $|\phi_{\alpha,l}\rangle$ denotes Eve's probe states. That way, because of the introduced entanglement, Alice's encoding operation also modifies the state of the ancilla. By inspection of the ancilla's state Eve can gain some information about the encoded message. On the other hand, Eve's attack operation inevitably breaks the perfect correlation of the 'travel' and 'home' qudits, and that violation can be detected when Alice and Bob switch to control mode in which they perform local measurements on the possessed qudits and classically communicate their results. Unfortunately, the control mode executed only in computational basis is insufficient, as Eve can mount an undetectable attack in which she can infer half the information posted by Alice [19, 23]. It has been also shown in [23] that the incorporation of dual basis removes such possibility. The question how protocol detectability can be improved by taking into account all possible mutually unbiased bases remains open.

Without loss of generality it may be assumed that Bob sends a state $|\alpha\rangle$ [2, 19]. It follows from (6) that $p_\alpha^{(0)} = |a_{\alpha,\alpha}|^2$ describes the non-detection probability when computational basis $\mathcal{B}^{(0)}$ is used in control mode. If Alice selects another basis $\mathcal{B}^{(m)}$ then the 'travel' qudit after attack is seen as

$$|\psi_\alpha\rangle = A|b_\alpha^{(0)}, \phi\rangle = \sum_{k=0}^{N-1} c_{\alpha,k} |b_k^{(m)}\rangle, \phi_{\alpha,k}\rangle, \quad (7)$$

where $c_{\alpha,k} = \sum_{l=0}^{N-1} a_{\alpha,l} \langle b_k^{(m)} | b_l^{(0)} \rangle$. The attack is not detected in the basis $\mathcal{B}^{(m)}$ with probability

$$p_\alpha^{(m)} = |c_{\alpha,\alpha}|^2 = \left| \langle b_\alpha^{(m)} | a_{\alpha,\cdot} \rangle \right|^2, \quad (8)$$

where $|a_{\alpha,\cdot}\rangle = \sum_{l=0}^{N-1} a_{\alpha,l} |b_l^{(0)}\rangle$. The non-detection probability averaged over multiple control mode cycles is given by

$$d_\alpha = \sum_{m=0}^{M-1} q_m p_\alpha^{(m)}, \quad (9)$$

where M is the number of bases and q_m describes relative frequency of their selection.

It should be shown for completeness that in the control mode Bob can unambiguously infer Alice's local measurement result as long as he is informed about the used basis. This follows from the fact that, as the local change of basis does not influence the entanglement, the measurement performed by Alice fully determines the outcome of Bob's measurement. Let us suppose that Alice performed a measurement in the basis \mathcal{B} and obtained symbol i . In this case, the state of the system, after the projective measurement, reads

$$\begin{aligned} (|U_i\rangle \langle U_i| \otimes \mathbb{I}) \left(\sum_k |k\rangle \otimes |k\rangle \right) &= |U_i\rangle \otimes \left(\sum_k \langle U_i | k \rangle |k\rangle \right) \\ &= |U_i\rangle \otimes |\overline{U_i}\rangle, \end{aligned} \quad (10)$$

where U_i is i^{th} vector of the basis \mathcal{B} . From the above one can notice that, if Bob performs a measurement in the basis $\overline{\mathcal{B}}$, he will obtain the symbol i with probability 1.

III. BOUNDS ON THE NON-DETECTION PROBABILITY

Let us begin with general theorem concerning non-detection probability.

Theorem 1. *Let $\{\mathcal{B}^{(0)}, \mathcal{B}^{(1)}, \dots, \mathcal{B}^{(M)}\}$ be a set of $M+1$ orthonormal bases, used in the control mode of the protocol and selected equally frequently. Then, the upper bound*

for the average non-detection probability (9) is given by

$$d_\alpha \leq \frac{1}{M+1} \sigma_1^2(V^{(\alpha)}), \quad (11)$$

where $\sigma_1(V^{(\alpha)})$ denotes the greatest singular value of $V^{(\alpha)} = \left\{ \overline{B}_{\alpha,j}^{(i)} \right\}_{ij}$.

Proof. Let us denote by v_m the α^{th} element of $\mathcal{B}^{(m)}$. By $V^{(\alpha)}$ we denote a matrix with rows given by bra vectors $\langle v_m|$, i.e. $V_{m,j}^{(\alpha)} = \overline{B}_{\alpha,j}^{(m)}$ (overline denotes complex conjugate). If control bases are selected equally frequently the average non-detection probability (9) can be written as

$$d_\alpha = \frac{1}{M+1} \left\| V^{(\alpha)} |a_{\alpha,\cdot}\rangle \right\|^2, \quad (12)$$

and since $\max_{|x\rangle} \|V^{(\alpha)}|x\rangle\|^2 = \sigma_1^2(V^{(\alpha)})$ we obtain the result. \square

Let us now assume that the control mode is executed in $M+1$ mutually unbiased bases. In this case the upper bound on the non-detection probability is stated in the following theorem.

Theorem 2. *If the control mode is executed in $M+1$ mutually unbiased bases, then the average non-detection probability is bounded by*

$$d_\alpha \leq \frac{1 + M/\sqrt{N}}{1 + M}. \quad (13)$$

Proof. Let us introduce a matrix $W = V^{(\alpha)} V^{(\alpha)\dagger}$ where $V^{(\alpha)}$ is defined as in the proof of Theorem 1. Directly from the definition of matrix $V^{(\alpha)}$ and MUB condition (1) we get

$$W_{i,j} = \langle v_i | v_j \rangle = \{ \delta_{i,j} + (1 - \delta_{i,j}) e^{i\phi_{i,j}} / \sqrt{N} \}_{i,j=0}^M. \quad (14)$$

Note that matrix W does not depend on the particular α . The maximal singular value of the matrix W can be bounded as [16] (see also inequality [11, Eq. (3.7.2)])

$$\sigma_1(W) \leq \left((\max_i \sum_j |W_{i,j}|) (\max_j \sum_i |W_{i,j}|) \right)^{1/2}. \quad (15)$$

Taking into account (14) we get

$$\max_i \sum_j |W_{i,j}| = \max_j \sum_i |W_{i,j}| = 1 + M/\sqrt{N}, \quad (16)$$

and the result follows from Theorem 1 and the fact that $\sigma_1^2(V^{(\alpha)}) = \sigma_1(W)$. \square

In the case of dimension $N = p^m$ for prime p and m being a positive integer, there exists a set of $N+1$ mutually unbiased bases [7], and the bound (13) reads

$$d_\alpha \leq \frac{1 + \sqrt{N}}{1 + N}. \quad (17)$$

It is possible to improve this bound using explicit expression (2).

Theorem 3. *Let $N = p^m$ where p is an odd prime and m is a positive integer. Then the maximal non-detection probability is bounded by*

$$d_\alpha \leq \frac{3}{1 + N}. \quad (18)$$

Proof. Let us introduce matrix $W = V^{(\alpha)\dagger} V^{(\alpha)}$ for some fixed α

$$W_{\mu,\nu} = \sum_{q=0}^N (V^{(\alpha)\dagger})_{\mu,q} V_{q,\nu} = \sum_{q=0}^N B_{\alpha,\mu}^{(q)} \overline{B}_{\alpha,\nu}^{(q)}. \quad (19)$$

Matrix W may be decomposed as $W = P + Q$:

$$P_{\mu,\nu} = B_{\alpha,\mu}^{(0)} \overline{B}_{\alpha,\nu}^{(0)} = \delta_{\alpha,\mu} \delta_{\alpha,\nu}, \quad (20)$$

$$\begin{aligned} Q_{\mu,\nu} &= \sum_{q=1}^N B_{\alpha,\mu}^{(q)} \overline{B}_{\alpha,\nu}^{(q)} \\ &= \omega^{\ominus \alpha \odot (\mu \ominus \nu)} \frac{1}{N} \sum_{q=1}^N \omega^{(q-1) \odot (\mu \odot \mu \ominus \nu \odot \nu) \odot 2} \\ &= \omega^{\ominus \alpha \odot (\mu \ominus \nu)} \delta_{\mu \odot \mu \ominus \nu \odot \nu, 0}, \end{aligned} \quad (21)$$

where we have used identities $\omega^{k\omega^l} = \omega^{k\oplus l}$ and $\sum_{k=0}^{N-1} \omega^{k\odot l} = N\delta_{l,0}$ (see eg. [7]). Thus, $|Q_{\mu,\nu}| = \delta_{(\mu \ominus \nu) \odot (\mu \oplus \nu), 0}$ and using bound (15) we get $\sigma_1(Q) \leq 2$. Obviously $\sigma_1(P) = 1$. Thesis follows from (11) combined with $\sigma_1^2(V) = \sigma_1(W)$ and inequality [11, Eq. (3.3.17)]

$$\sigma_1(P + Q) \leq \sigma_1(P) + \sigma_1(Q) = 3. \quad (22)$$

\square

It has been shown that usage of at least two dual bases is sufficient to ensure asymptotic protocol security [23]. However, the detection capabilities of the control mode are significantly improved when more mutually unbiased bases are used. This follows from the comparison of the bound on average non-detection probability obtained in [23] (curve (d) on Fig. 1) with the bounds obtained herein (curves (b) to (d)). The improvement of the protocol's detectability becomes more apparent with the increase of the dimension of the underlying Hilbert space – for bound from [23] we have $\lim_{N \rightarrow \infty} d_{\max} = 1/2$ while for (17) and (18) $\lim_{N \rightarrow \infty} d_{\max} = 0$. Although the asymptotic behavior of the bounds (17) and (18) is similar, they differ in the provided optimality.

The comparison of the considered bounds with numerical results is presented in Fig. 1. It follows that bound (18) is close to optimal. It was also verified that the best fitting to numerical estimates is achieved for $\sigma_1^2(V) = \frac{1}{2}(3 + \sqrt{5}) \approx 2.618$.

Further improvement can be proposed based on the analysis of the proof of Theorem 3. The matrix P is related to the control mode tests executed in the computational basis. If that basis is excluded from the control mode, one obtains a better protocol behaviour. We can state the following.

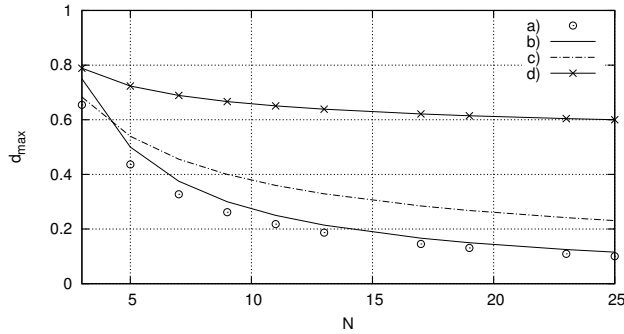


FIG. 1: Comparison of upper bounds on average probability of non-detection calculated: a) via numerical simulations, b) with expression (18), c) with expression (17), d) when only two bases are used in control mode [23] ($d_{\max} = (1 + 1/\sqrt{N})/2$).

Corollary 1. *Let us assume, that $N = p^m$, where p is an odd prime and m is a positive integer, and the computational basis is excluded from the control mode. In this case an average non-detection probability is bounded by*

$$d_{\alpha} \leq 2/N. \quad (23)$$

It should be noted that, as the information is encoded and decoded in the computational basis, Eve still has to use this basis for an attack preparation. Comparing the above bound with the numerical estimate for the seminal protocol, we observe about 30% improvement in an attack detection capabilities.

IV. CONCLUSIONS

In this paper we have proposed an extended version of the ping-pong protocol, which incorporates the usage of mutually unbiased bases in the control mode. We provided upper bounds on eavesdropping average non-detection probability in the proposed protocol.

If the communicating parties use $M + 1$ mutually unbiased bases in the control mode, the bound is given by the leading singular value of the matrix with rows given by the appropriate bra vectors. One should note that the number M of bases used in the control mode should depend on the dimension.

If the communicating parties use particles of dimension $N = p^m$, where p is an odd prime and m is a positive integer, it is possible to provide a better estimate. Assuming that Alice and Bob use $N + 1$ bases and construct them according to [7], the non-detection probability averaged over sufficiently many cycles never exceeds $3/(N + 1)$. Eavesdropping detection capabilities can be improved by the exclusion of the computational basis from the control mode.

Acknowledgments

This work was supported by the Polish National Science Centre under the research project N N516 475440. The authors would like to thank K. Życzkowski and P. Gawron for interesting discussions.

-
- [1] Almut Beige, Berthold Georg Englert, Christian Kurt-siefer, and Harald Weinfurter. Secure communication with a publicly known key. *Act. Phys. Pol.*, 101(3):357–368, 2002.
 - [2] K. Boström and T. Felbinger. Deterministic secure direct communication using entanglement. *Phys. Rev. Lett.*, 89(18):187902, 2002.
 - [3] Stephen Brierley, Stefan Weigert, and Ingemar Bengtsson. All mutually unbiased bases in dimensions two to five. *Quant. Inf. Comput.*, 10:0803–0820, 2010.
 - [4] Qing-Yu Cai and Bai-Wen Li. Deterministic secure communication without using entanglement. *Chin. Phys. Lett.*, 21(4):601–603, 2004.
 - [5] Qing Yu Cai and Bai Wen Li. Improving the capacity of the Boström-Felbinger protocol. *Phys. Rev. Lett.*, 69(5):054301, May 2004.
 - [6] Fu-Guo Deng, Xi-Han Li, Chun-Yan Li, Ping Zhou, and Hong-Yu Zhou. Quantum secure direct communication network with einstein-podolsky-rosen pairs. *Phys. Lett. A*, 359(5):359 – 365, 2006.
 - [7] T. Durt. About mutually unbiased bases in even and odd prime power dimensions. *J. Phys. A: Math. Gen.*, 38:5267, 2005.
 - [8] T. Durt, B.-G. Englert, I. Bengtsson, and K. Życzkowski. On mutually unbiased bases. *Int. J. Quantum Inf.*, 8(4):535–640, 2010.
 - [9] Thomas Durt, Dagomir Kaszlikowski, Jing-Ling Chen, and L. C. Kwek. Security of quantum key distributions with entangled qudits. *Phys. Rev. A*, 69(3):032313, Mar 2004.
 - [10] A. Eusebi and S. Mancini. Deterministic quantum distribution of a d-ary key. *Quantum Inform. Comput.*, 9(11 & 12):950–962, 2009.
 - [11] R. A. Horn and C. R. Johnson. *Topics in Matrix Analysis*. Cambridge University Press, 1991.
 - [12] O. Korchenko, Y. Vasiliu, and S. Gnatyuk. Modern quantum technologies of information security against cyberterrorist attacks. *Aviation*, 14(2):58–69, 2010.
 - [13] X. S. Liu, G. L. Long, D. M. Tong, and Feng Li. General scheme for superdense coding between multiparties. *Phys. Rev. A*, 65(2):022304, Jan 2002.
 - [14] Marco Lucamarini and Stefano Mancini. Secure deterministic communication without entanglement. *Phys. Rev. Lett.*, 94:140501, Apr 2005.
 - [15] Daniel McNulty and Stefan Weigert. All mutually unbiased product bases in dimension six. <http://arxiv.org/abs/1111.3632v1>, 2011.
 - [16] J. Schur. Bemerkungen zur theorie der beschränkten bilinearformen mit unendlich vielen veränderlichen. *J. Reine Angew. Math.*, 1911(140):1–28, 1911.

- [17] Guo-Fang Shi, Xiao-Qiang Xi, Ming-Liang Hu, and Rui-Hong Yue. Quantum secure dialogue by using single photons. *Opt. Commun.*, 283(9):1984 – 1986, 2010.
- [18] Kaoru Shimizu, Kiyoshi Tamaki, and Hiroyuki Fukasaka. Two-way protocols for quantum cryptography with a nonmaximally entangled qubit pair. *Phys. Rev. A*, 80(2):022323, Aug 2009.
- [19] Eugene V. Vasiliu. Non-coherent attack on the ping-pong protocol with completely entangled pairs of qutrits. *Quantum Inf. Process.*, 10:189–202, 2011.
- [20] E.V. Vasiliu and S.V. Nikolaenko. Synthesis of the secure system of direct message transfer based on the ping-pong protocol of quantum communication. *Scientific works of the Odessa national academy of telecommunications named after O.S. Popov*, (1):83–91, 2009. (in Russian).
- [21] Chuan Wang, Fu-Guo Deng, Yan-Song Li, Xiao-Shu Liu, and Gui Lu Long. Quantum secure direct communication with high-dimension quantum superdense coding. *Phys. Rev. A*, 71:044305, 2005.
- [22] Jian Wang, Quan Zhang, and Chao-Jing Tang. Quantum secure direct communication based on order rearrangement of single photons. *Phys. Lett. A*, 358(4):256 – 258, 2006.
- [23] Piotr Zawadzki. Security of ping-pong protocol based on pairs of completely entangled qudits. *Quantum Inf. Process.*, 2011. (published online).
- [24] Piotr Zawadzki. Improving security of the ping-pong protocol. *Quantum Inf. Process.*, 2012. (published online).
- [25] You-Bang Zhan, Ling-Ling Zhang, and Qun-Yong Zhang. Quantum secure direct communication by entangled qutrits and entanglement swapping. *Opt. Commun.*, 282(23):4633 – 4636, 2009.